UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/588,460	08/04/2006	David Naccache	1032326-000404	5746

21839 7590 04/15/2009
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
VAUGHAN, MICHAEL R	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
04/15/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com

Office Action Summary	Application No.	Applicant(s)	
	10/588,460	NACCACHE, DAVID	
	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 March 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

The instant application having Application No. 10/588460 is presented for examination by the examiner. Claims 1-15 are amended and remain pending.

Response to Amendment

Claim Objections

The current amendments are sufficient in overcoming the previous objections.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The new amendments introduce indefiniteness in the claimed invention.

As per claims 1, 2, and 5, it seems the steps of securing assess in authenticating a user are a mix of registration templates and the actual steps during when a user who has previously registered seeks to gain access. Examiner is unsure if this is the case

and which steps precisely belong to either situation. For example the step of obtaining is interpreted to occur when a user is trying to gain access because of the recitation "for every access request...said party requesting access". The next step "encryption step" is storing a authentic biometric signature. For it to be authentic, it must be assumed this step occurred during registration. A newly acquired sample would not be deemed authentic without first authenticating it. Further indefiniteness steps from this step because it is named an encryption step, however only storing explicitly occurs in the step. The encryption seems to occur in a later step in the claim. However said encryption is mentioned as happening in a prior [unknown] step so it is assumed again that the storing of an encrypted version occurred during registration of the party. The next step could be interpreted as happening during registration or during requesting access. The notion that the party is authorized is loosely coupled to the personal identification code by the word attributed so its unclear whether the party is yet authorized. For sake of examination, Examiner will interpret this limitation to occur during registration as well. The matching step will also be interpreted as happening during registration as well. However the final steps occur during requesting access.

From these aforementioned problems the scope of the invention is not distinctly pointed out. The mixing of the registration steps within the access attempt is confusing. It would be clearer if the registration steps were distinctly separate in the claim from the requesting access steps. Logically, it is true that registration occurs prior to requesting access. The party's identifying data must first be acquired and stored so that when the

request for access happens, the newly acquired samples can be matched to the stored data. The dependent claims are likewise rejected for at least the same reasons.

Appropriate correction is required.

Response to Arguments

Applicant's arguments filed 3/23/09 have been fully considered but they are not persuasive. First of all the problems mentioned under the 112 rejection cause some confusion in understanding what is claimed. However the newly amended limitations are interpreted as occurring during registration of a party for the reasons listed above. With that interpretation, Examiner respectfully disagrees with Applicant's allegation that Watanabe fails to teach the newly amended claims. It is evident from Figure 5 which shows the information stored during registration of a user that both the user ID of the subject (personal identification number) and the encrypted subject template (authentic biometric signature) are matched together into a certificate of the registering party. Also see paragraph 0209. For more evidence of the relationship between the user ID and the biometric template, see figures 40 and 41 where the user submits his/her user ID with the biometric input sampling. This occurs when the user is requesting access which supports the fact that during registration this information was collected and put together. It is a way of checking to make sure the party which might guess an ID possesses the correct biometrics.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-15 are rejected under 35 U.S.C. 102(b) as being anticipated by USP Application Publication 2002/0069361 to Watanabe et al., hereinafter Watanabe.

As per claim 1, Watanabe teaches a method of securing access to a piece of equipment [PC], this method comprising at least one attribution operation consisting of supplying a reference datum to an authentication medium (237);

an acquisition operation consisting of obtaining, for every access request formulated by a party requesting access to the equipment, a biometric signature of this said party requesting access (238);

an encryption step storing an encrypted version of at least one authentic biometric signature (0209);

a receiving step receiving and storing a personal identification code attributed to the party authorized to access the piece of equipment (Fig. 5 and 0214);

a matching step matching the stored personal identification code with the stored encrypted version of the at least one authentic biometric signature (combined together in Figure 5); and

and a verification step consisting of verifying, by means of the reference datum, the authenticity of the biometric signature obtained from the party requesting access, further including a prior encryption step, during which an encrypted version of at least one authentic biometric signature belonging to at least one person authorized to access the piece of equipment is created (250), wherein the verification step comprises a decryption operation implemented in the authentication medium and consisting of which includes decrypting, by means of a secret key, the encrypted version of an authentic biometric signature supplied to this said authentication medium as a reference datum during the access request, and in that wherein the verification step comprises a comparing operation implemented by secretly comparing the biometric signature obtained from the party requesting access during the access request with the authentic biometric signature that results from the decryption step (238).

As per claim 2, Watanabe teaches an electronic card having at least one decryption module using a secret [private] key (356-357) said electronic card performing the following steps:

receiving a reference datum to an authentication medium (237);

obtaining, for every access request formulated by a party requesting access to the equipment, a biometric signature of this said party requesting access (238);

storing an encrypted version of at least one authentic biometric signature (0209);

receiving and storing a personal identification code attributed to the party authorized to access the piece of equipment (Fig. 5 and 0214);

matching the stored personal identification code with the stored encrypted version of the at least one authentic biometric signature (combined together in Figure 5); and

verifying, by means of the reference datum, the authenticity of the biometric signature obtained from the party requesting access, further including a prior encryption step, during which an encrypted version of at least one authentic biometric signature belonging to at least one person authorized to access the piece of equipment is created (250), wherein the verification step comprises a decryption operation implemented in the authentication medium and consisting of which includes decrypting, by means of a secret key, the encrypted version of an authentic biometric signature supplied to this said authentication medium as a reference datum during the access request, and in that wherein the verification step comprises a comparing operation implemented by secretly comparing the biometric signature obtained from the party requesting access during the access request with the authentic biometric signature that results from the decryption step (238).

As per claim 3, Watanabe teaches a comparison module (357).

As per claim 4, Watanabe teaches an encryption module (232).

As per claim 5, Watanabe teaches a device [IC card] for securing access to a piece of equipment [shared user device], this device comprising: an authentication medium [terminal] which is supplied with a reference datum [IDC]; a sensor [sampling information acquisition apparatus] obtaining, during every access request formulated by

a party requesting access to the equipment, a biometric signature of said party requesting access (357);

A computer storing an encrypted version of at least one authentic biometric signature (0209);

receiving and storing a personal identification code attributed to the party authorized to access the piece of equipment (Fig. 5 and 0214);

matching the stored personal identification code with the stored encrypted version of the at least one authentic biometric signature (combined together in Figure 5);

and a controller included in the authentication medium and selectively authorizing the party requesting access to access the piece of equipment in accordance with the result of a verification of the authenticity of the biometric signature of the party requesting access by means of the reference datum (356)

wherein the controller comprises a decryption module and a comparison module wherein the reference datum supplied to the authentication medium consists of comprises an encrypted version of an authentic biometric signature allegedly attributed to the party requesting access (356), wherein the decryption module uses a secret [private] key by means of which it secretly reconstructs (356), upon each access request, the authentic biometric signature from its encrypted version, and wherein the comparison module secretly compares the biometric signature obtained from the party requesting access with the reconstructed authentic biometric signature, and supplies a comparison result that constitutes the result of the verification (357).

As per claim 6, Watanabe teaches the authentication medium is a card, equipped with a memory that cannot be read from outside, in which the secret key is stored (355-356).

As per claim 7, Watanabe teaches at least one computer makes up at least a part of the equipment to which the access is secured (shared user device is a computer 237).

As per claim 8, Watanabe teaches the computer contains in its memory [database] a plurality of personal identification codes [personal information] attributed to a corresponding plurality of persons authorized to access the equipment and associated with a corresponding plurality of encrypted authentic biometric signatures [IDA] for these authorized persons, and wherein the computer delivers to the identification medium, when receiving an access request, the encrypted authentic biometric signature that corresponds to the identification code supplied by the party requesting access, such that a single authentication medium provides several persons with secure access to the computer (248-250).

As per claim 9, Watanabe teaches an encryption module that delivers an encrypted version of an authentic biometric signature supplied in plain form by the sensor in response to an encryption command (250).

As per claim 10, Watanabe teaches the secret key is a private key with a matching public key, and wherein the encryption module is included in the computer and uses the public key (250).

As per claim 11, Watanabe teaches an encryption module (250).

As per claim 12, Watanabe teaches at least one computer that makes up at least a part of the equipment to which the access is secured (237 and 295).

As per claims 13, 14, and 15, Watanabe teaches an encryption module that delivers an encrypted version of an authentic biometric signature supplied in plain form by the sensor in response to an encryption command (248-250).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2431